Exhibit 2

Trials@uspto.gov
571-272-7822

Paper 8
Entered: May 22, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

IPR2024-00003
Patent 9,198,117 B2

Before GARTH D. BAER, STEPHEN E. BELISLE, and RUSSELL E. CASS, *Administrative Patent Judges.*

CASS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Samsung Electronics Co., Ltd. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–18 (the "challenged claims") of U.S. Patent No. 9,198,117 B2 (Ex. 1001, "the '117 patent"). Paper 2, 1 ("Pet."). Headwater Research LLC ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

An *inter partes* review may not be instituted unless it is determined that "the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314 (2018); *see also* 37 C.F.R § 42.4(a) (2021) ("The Board institutes the trial on behalf of the Director."). The reasonable likelihood standard is "a higher standard than mere notice pleading," but "lower than the 'preponderance' standard to prevail in a final written decision." *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29, 13 (PTAB Dec. 20, 2019) (precedential).

For the reasons provided below and based on the record before us, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we do not institute an *inter partes* review on all grounds set forth in the Petition.

B. Real Parties in Interest

Petitioner states that the real parties in interest are Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. Pet. 105.

Patent Owner states that Headwater Research LLC is the real party in interest. Paper 4, 2.

C. Related Proceedings

The parties indicate that the '117 patent is the subject of the following district court case: *Headwater Research LLC v. Samsung Electronics Co., Ltd.*, No. 2:23-cv-00103 (E.D. Tex.). Pet. 105; Paper 4, 2.

D. The '117 Patent (Ex. 1001)

The '117 patent relates to a "network system with [a] common secure wireless message service serving multiple applications on multiple wireless devices." Ex. 1001, code (54). The '117 patent explains that "[e]ach of several mobile end user devices contains a device messaging agent that securely communicates with a network message server over a wireless network." *Id.* at code (57). The network message server "delivers messages to the device messaging agent on behalf of a plurality of network application servers," each of which "supplies the network message server with application data and an indication of a device and an application on the device to which the application data should be delivered." *Id.* The network message server then "securely passes the data and an application identifier to the device messaging agent on the appropriate mobile end-user device." *Id.* The device messaging agent then "maps the application identifier to a software process corresponding to the application, and a secure interprocess communication service delivers the application data to that software process." *Id.*

E. Illustrative Claim

Of challenged claims 1–18, claim 1 is independent. For purposes of the issues raised at this stage of the proceeding, claim 1 is illustrative and is reproduced below.

> [1pre] A network system comprising:
>
> [1.1] a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network; and
>
> [1.2] a network message server supporting a plurality of secure Internet data connections, each secure Internet data connection between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network,
>
> [1.3] the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications,
>
> [1.4] the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests, and
>
> [1.5] the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request;
>
> [1.6] each device messaging agent, when executing, to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent, and

> [1.7] to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.

Ex. 1001, 163:46–164:16 (indents and bracketed paragraph identifiers added).

F. Applied References

Petitioner relies upon the following references:

Houghton, WO 2006/077283 A1, published Jul. 27, 2006 (Ex. 1005, "Houghton");

Kalibjian, US 2007/0011736 A1, published Jan. 11, 2007 (Ex. 1006, "Kalibjian");

Munson, US 2009/0240807 A1, published Sep. 24, 2009 (Ex. 1007, "Munson");

Rakic, US 2009/0282256 A1, published Nov. 12, 2009 (Ex. 1008, "Rakic");

Anderson, *Security Engineering*, second edition, copyright 2008 (Ex. 1010, "Anderson");

Lee, WO 2008/048075 A1, published Apr. 24, 2008 (Ex. 1012, "Lee");

Ellison, US 7,082,615 B1, issued Jul. 25, 2006 (Ex. 1013, "Ellison");

Hämäläinen, US 2007/0214245, published Sep. 13, 2007 (Ex. 1018, "Hämäläinen").

Pet. iii–iv, 2. Petitioner also submits the Declaration of Dr. Patrick Traynor (Ex. 1003). Patent Owner submits the Declaration of Dr. Michael Brogioli (Ex. 2001).

G. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–18 of the '117 patent based on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3–13	103(a)[1]	Houghton, Kalibjian
2, 16–18	103(a)	Houghton, Kalibjian, Munson
14, 15	103(a)	Houghton, Kalibjian, Rakic
1, 3–6, 9–11, 13–15	103(a)	Lee, Ellison, Anderson
2, 16–18	103(a)	Lee, Ellison, Anderson, Hämäläinen
7, 8, 12	103(a)	Lee, Ellison, Anderson, Houghton

Pet. 1.

II. DISCUSSION

A. Claim Construction

A claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b)." 37 C.F.R. § 42.100(b). At this stage of the proceeding, neither party presents any claim terms for construction. Pet. 2–3; Prelim. Resp. 5. Based on the present record, we determine that it is not necessary to provide an express interpretation of any claim terms for

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), included revisions to 35 U.S.C. § 103 that became effective after the filing of an application to which the '117 patent claims priority. For purposes of this Decision, we apply the pre-AIA version of 35 U.S.C. § 103.

purposes of this Decision. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1374 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). We address claim interpretation, to the extent necessary, in our obviousness analysis below.

B. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.[2] *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

[2] At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic, Inc. v. Avid Technology, Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

Petitioner introduces the testimony of Dr. Traynor that a person of ordinary skill in the art would have had "(1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) 3–5 years of experience in services and application implementation in communication networks." Pet. 3 (citing Ex. 1003 ¶¶ 21–22). Petitioner further states that "[a]dditional graduate education could substitute for professional experience, and *vice versa*." *Id.* Patent Owner states that "[f]or purposes of this preliminary response," it "does not challenge that definition." Prelim. Resp. 5.

For purposes of this Decision, we adopt the assessment of the level of ordinary skill in the art proposed by Petitioner and Dr. Traynor and not disputed by Patent Owner as reasonable and consistent with the prior art. *See Okajima v Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir 2001) (the prior art may reflect an appropriate level of skill in the art).

D. Ground 1A:[3] Asserted Obviousness of Claims 1 and 3–13 Based on Houghton in view of Kalibjian

Petitioner contends that claims 1 and 3–13 would have been obvious over Houghton in view of Kalibjian. Pet. 5–50. Patent Owner disagrees, arguing that Petitioner has failed to establish that these claims would have been obvious based on Houghton and Kalibjian. Prelim. Resp. 6–16.

1. Overview of Houghton (Ex. 1005)

Houghton discloses "[a] server outside a wireless network security entity" that "is adapted to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message." Ex. 1005, code (57). The mobile terminal includes software "which initiates and maintains contact with the server using Internet technologies," which "allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time." *Id.* More specifically, Houghton discloses a "push client 405" that "is preferably implemented in the form of . . . software run in a processor of the mobile terminal 404" and that this mobile terminal may be "a commercially available mobile terminal, such as a portable phone or appliance capable of running software or personal digital assistant, which provides a platform for downloading application software over air or from a personal computer, installing the software in the terminal, and running the software in the terminal." *Id.* at 16:21–29.

[3] Here, and elsewhere in the Decision, the identification of the grounds using designations such as "Ground 1A" and "Ground 1B" refers to the designation of the grounds as presented in the Petition.

Houghton also discloses the use of various "network parameters" for establishing the connection between the mobile terminal and the server. Ex. 1005, 18:16–27. These "network parameters" may include the "[u]se of a secure protocol such as HTTPS, IP-Sec, secure IP6 or a proprietary security protocol to identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties." *Id.* at 19:14–17. Houghton also discloses that "a data connection between application server 802 and mobile application 804 is established" with the aid of a "persistent managed, tested and configured data connection . . . between push server 401/801 and push client 405/804." *Id.* at 23:3–9. Additionally, Houghton describes an "IP or other API (application programming interface) connection between application server 802 and push server 801," which "simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure." *Id.* at 23:9–12.

2. Overview of Kalibjian (Ex. 1006)

Kalibjian discloses "policy protected cryptographic Application Programming Interfaces (APIs) that are deployed in secure memory." Ex. 1006, code (57). One embodiment of Kalibjian's invention is "a method of software execution" that "includes executing an application in a first secure memory partition; formatting a request to comply with a pre-defined secure communication protocol; transmitting the request from the application to a cryptographic application programming interface (API) of the application" in "a second secure memory partition that is separate and secure from the first secure memory portion; and verifying, in the second secure memory partition, that the request complies with a security policy

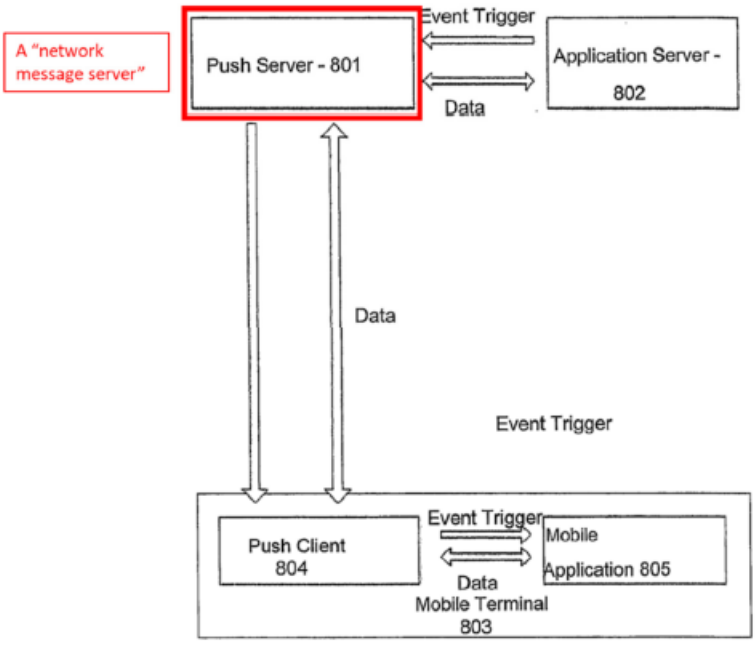
before executing the request." *Id.* Specifically, when an application makes a request, a "policy checking algorithm 224 evaluates the request with respect to the established security policy" and, "[i]f the request is valid (i.e., the request does not violate one or more rules of the security policy), then the request is carried-out, executed, or permitted." *Id.* ¶ 21. These security policies can include "cryptographic algorithms to use, key sizes, allowable hash algorithms, etc." *Id.*

3. Analysis of Independent Claim 1

The parties dispute whether the proposed combination teaches limitation [1.3] of claim 1, which recites "a network message server" that is "configured to receive, from each of the plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications." Ex. 1001, 163:57–62.

Petitioner argues that Houghton's "push server," such as push server 801[4], is a "network message server in communication with push clients." Pet. 17 (citing Ex. 1005, 8:14–32, 16:16–35, 17:1–12, 21:35–36, 22:1–6, 24:19–34, Figs. 2–5, 7–9). Petitioner presents an annotated version of Houghton's Figure 8 showing push server 801 communicating with a push client 804 executing on a mobile terminal 803, reproduced below.

[4] Petitioner notes that "Houghton also refers to push servers as components 202, 301, 401, 501, 701, and 901." Pet. 17 n.5.



Petitioner's annotated version of Houghton's Figure 8 showing push sever 801 as the claimed "network message server" communicating with push client 804 executing on mobile terminal 103. Pet. 17 (citing Ex. 1005, Fig. 8; Ex. 1003 ¶ 41).

Petitioner also asserts that Houghton's push server 701 implements "a 'COMMAND PUSH' (hereinafter, 'command push') process in which an 'application server 702' pushes an 'application command message' to a push client executing on the mobile terminal." Pet. 20–21 (citing Ex. 1005, 21:35–36, 22:1–18, Fig. 7). Additionally, according to Petitioner, this command push process is "triggered by a trigger event as for example . . . application server 702 to push an application command message to the push client 704," which satisfies the claim language requiring that the network message server is "configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data." *Id.* at 21 (citing Ex. 1005, 16:15–21, 21:35–36, 22:1–18, Fig. 7; Ex. 1003 ¶ 46) (alteration in original). Petitioner further contends that "[t]rigger events include desired application functions (e.g., 'an alarm, notification, or

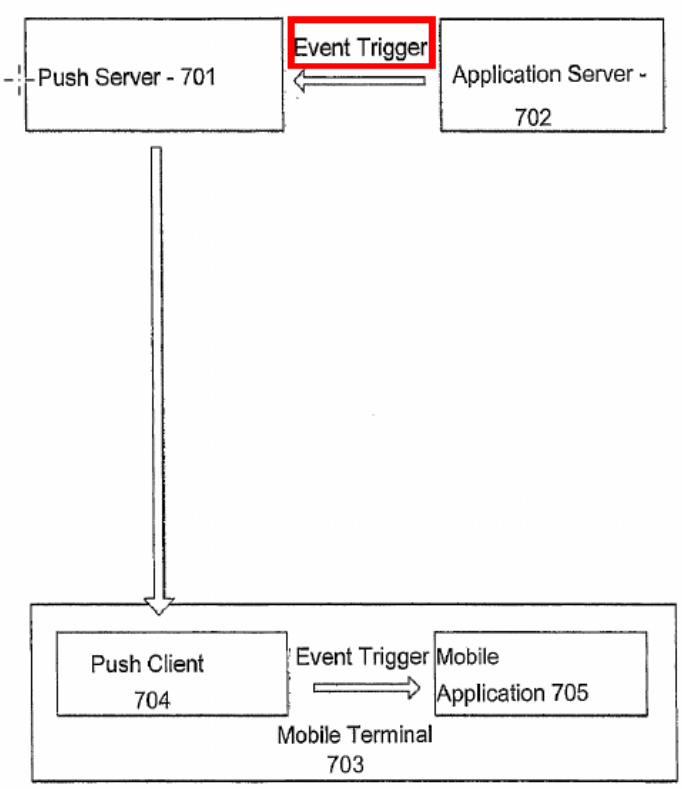
measurement result'), which the push server packages into messages and transmits to the push client 405 (such that the messages are '***based on***' the trigger events)." *Id.* at 24 (citing Ex. 1005, 19:25–34).

Petitioner also argues that "Houghton discloses that command messages 'initiate a mobile terminal client trigger event in a mobile application from a plurality of such applications' and that '[e]ach mobile application 205 has a fixed IP port number such as TCP/IP or UDP/IP' used to route the message to the application," which satisfies the claim language reciting "each such request indicating . . . one of a plurality of applications." Pet. 21 (citing Ex. 1005, 8:14–26, 21:35–36, 22:1–18, Figs. 7–8) (emphasis omitted, alteration in original). For this assertion, Petitioner relies on the testimony of Dr. Traynor that one of ordinary skill "would have recognized that 'IP port numbers' would have additionally been unique to the mobile terminal" (which satisfies the claim language "each such request indicating a corresponding one of the mobile end-user devices"), as "IP addresses were (and still are) used as of the Critical Date to differentiate network locations (e.g., one mobile terminal from another)." *Id.* (citing Ex. 1003 ¶ 46). Petitioner further contends that "Houghton corroborates Dr. Traynor's testimony" by disclosing "that 'IP-based technologies' use 'IP address[es]' to indicate a particular terminal to receive a mobile push." *Id.* (citing Ex. 1005, 1:10–18, 6:5–18; Ex. 1003 ¶ 46). Additionally, Petitioner argues, "Houghton's push messages include '[a]dditional binary or text application specifying which mobile application 406 from a plurality of such applications.'" *Id.* at 24 (citing Ex. 1005, 21:7–34; Ex. 1003 ¶ 48).

Relying on Dr. Traynor, Petitioner also argues that one of ordinary skill "would have recognized or found obvious that the network message

server would receive requests from a '***plurality of network application servers***' as this was well known in the art by the Critical Date." Pet. 22 (citing Ex. 1003 ¶ 47). "Indeed," Petitioner asserts, "Houghton describes a plurality of 'content and application producers.'" *Id.* (citing Ex. 1005, 14:28–31). "Moreover," Petitioner contends, "Kalibjian discloses that its 'host computer system 40' (in communication with computing devices 20 over network 30) includes a plurality of 'computers . . . , computer systems, mainframe computers, servers, distributed computing devices, and gateway computers.'" *Id.* (citing Ex. 1006 ¶¶ 14–15) (alteration in original). Additionally, although Munson is not relied on in Ground 1 and is only applied as part of Ground 2, Petitioner argues that, "Munson discloses a content push service in communication with a plurality of such application servers." *Id.* (citing Ex. 1007, 1:48–56, 3:7–39, Figs. 1–2; Ex. 1003 ¶ 47).

Patent Owner responds that Petitioner's theory is deficient "because it speaks[,] at most, to what the ***command message sent from push server*** 701 to push client 704 indicates," and "says nothing about what the ***trigger events*** (i.e., the alleged 'requests') that are ***received by push server*** 701 from the application server [702] (i.e., 'from each of a plurality of application servers') indicate, which is what the Petitioner must show." Prelim. Resp. 12. Patent Owner presents an annotated version of Houghton's Figure 7, reproduced below, showing the trigger event sent from the application server to the push server.



Patent Owner's annotated version of Houghton's Figure 7 showing the event trigger sent from application server 702 to push server 701. Prelim. Resp. 9–10 (citing Ex. 1005, Fig. 7).

"Critically," Patent Owner contends, "the Petition only maps the 'push server' to the claimed 'network message server,' and never alleges that the 'push client' could be the claimed 'network message server.'" *Id.* at 12 (citing Pet. 17 (quoting Ex. 1005, Fig. 8)).

Additionally, according to Patent Owner, the Petition maps the claimed "network application server" to Houghton's application server, but Houghton's application server "does not send any messages to the push client at all, let alone claim limitation [1.3]'s 'request[s] indicating a corresponding one of the mobile end-user devices and one of a plurality of applications.'" Prelim. Resp. 13 (citing Pet. 21) (alteration in original). "In particular," Patent Owner argues, "the Petition does not provide ***any*** evidence or allegation that the ***trigger events received by the push server***

(i.e., the alleged 'requests' the alleged 'message server' is configured to receive) include IP address or port number information (or any other data allegedly indicating both a device and application)." *Id.* The "only discussion of the content of trigger events" in the Petition, according to Patent Owner, "merely alleges that these trigger events include information such as 'an alarm, notification, or measurement result,'" and "never contends that this information would include an IP address and port number (or any other information allegedly indicating both 'one of a plurality of applications' and 'a corresponding one of the mobile end-user devices')." *Id.* at 13–14 (citing Pet. 23–25).

Patent Owner further argues that "there is no need for the application server itself to provide both the IP address and port number information to the push server" because "the ***push server*** (not the application server) is involved in the 'persistent managed, tested, and configured data connection . . . between push server 401/801 and push client 405/804.'" Prelim. Resp. 14 (quoting Ex. 1005, 23:4–9). "The fact that the command message ***sent from*** the push server might be sent to an IP address and port number," according to Patent Owner, "does not mean that the trigger event ***received by*** the push server includes an IP address and port number." *Id.* (citing Ex. 2001 ¶ 42). Additionally, Patent Owner contends, the Petition does not "allege that the inclusion of IP address and port number information in the trigger events received by the push server would be inherent." *Id.* Moreover, Patent Owner asserts, "[b]ecause the push server manages the specifics of the connection, there is no reason that an application server would need to know the specific IP address and port number for the message that will ultimately be sent by the push server." *Id.*

at 15 (citing Ex. 2001 ¶ 43). Finally, Patent Owner argues that the Petition "includes no obviousness allegations with respect to the trigger event including IP address / port number information (or any other information allegedly indicating 'a corresponding one of the mobile end-user devices and one of a plurality of applications')." *Id.* at 16.

Based on the present record, we determine that Petitioner has failed to make a sufficient showing as to limitation [1.3] for purposes of institution. As Patent Owner notes, limitation [1.3] requires that "the network message server" is configured to receive multiple requests to transmit application data "indicating a corresponding one of the mobile end-user devices and one of a plurality of applications" from "each of a plurality of network application servers." Ex. 1001, 163:57–62. Petitioner maps the claimed "network message server" to Houghton's push server 801[5], and the "plurality of network application servers" to application server 702[6]. Pet. 17, 20. Petitioner also maps the claimed "multiple requests to transmit application data" from the network application servers to Houghton's "trigger event" that triggers "application server 702 to push an application command message to the push client 704"[7] (the "device messaging agent"). *Id.* at 13, 21. According to Petitioner, these "command messages" initiate "a mobile terminal client trigger event in a mobile application 705" running on a mobile terminal. *Id.* at 21.

---

[5] As noted above, Petitioner explains that "Houghton also refers to push servers as components 202, 301, 401, 501, 701, and 901." Pet. 17 n.5.
[6] Petitioner notes that "Houghton also refers to application servers as components 502, 802, and 902." Pet. 20 n.6.
[7] As noted above, Petitioner states that "Houghton also refers to push clients at components 704, 804, 904, and 906." Pet. 13 n.4.

Petitioner, however, does not sufficiently explain how Houghton teaches that the "network message server" (push server 701 or 801) is configured to receive requests from "each of a plurality of network application servers" (application servers 702 and 802) to transmit application data "indicating a corresponding one of the mobile end-user devices and one of a plurality of applications," as limitation [1.3] requires. Relying on Column 21, line 35 through Column 22, line 18, Petitioner argues that "Houghton discloses a 'COMMAND PUSH' . . . process in which ***an 'application server 702' pushes an 'application command message' to a push client*** executing on a mobile terminal." Pet. 20–21 (emphasis added). The cited portion of Houghton, however, does not state that ***application server 702*** pushes a command message to the push client, but rather states that ***push server 701*** carries out this step. As Houghton explains:

> Figure 7 illustrates an example of an 'COMMAND PUSH' procedure wherein ***the push server 701 is triggered by a trigger event as for example from an application server 702 to push an application command message to the push client 704*** and thereby initiate a mobile terminal client trigger event in a mobile application 705 from a plurality of such applications, program modules, and user interface features on the terminal 705.

Ex. 1005, 21:35–22:4 (emphasis added). As this passage from Houghton explains, it is push server 701, not application server 702, that sends the command message to push client 704. Application server 702 merely triggers push server 701 to send the command message.

Similar problems exist with Petitioner's assertion that, "[a]dditionally, Houghton discloses this command push process, implemented by a 'push server 701,' is '***triggered by a trigger event as for example . . . application server 702 to push an application command message to the push client***

704.'" Pet. 21 (emphasis added) (citing Ex. 1005, 16:15–21, 21:35–36, 22:1–18, Fig. 7; Ex. 1003 ¶ 46). As shown in the excerpt from page 22 of Houghton reproduced above, what Houghton actually says is that push server 701 "is triggered by a trigger event as for example ***from*** an application server 702 to push a command message to the push client 704." Ex. 1005, 21:36–22:2. By omitting the word "from" in its quotation, Petitioner suggests that Houghton discloses that an event trigger can involve application server 702, itself pushing an application command message to push client 704. What Houghton actually says, however, is that ***push server 701*** (not application server 702) pushes an application command message to push client 704. Houghton's "for example" language merely explains that the event trigger may be "from" an application server, not that the application server may push the command message to push client 704.

Thus, even if Petitioner is correct that Houghton discloses that the command messages pushed from push server 701 to push client 704 include IP port numbers "indicating a corresponding one of the mobile end-user devices and one of a plurality of applications," *see* Pet. 21, this is not sufficient to satisfy limitation [1.3], which requires that requests received from "network application servers" (mapped to application server 702) include this information. And, although application server 702 sends an event trigger to push server 701, Petitioner does not show that this event trigger includes information "indicating a corresponding one of the mobile end-user devices and one of a plurality of applications," as limitation [1.3] requires. Petitioner states that "trigger events" may include "an alarm, notification, or measurement result," but does not explain how this

information would indicate a corresponding mobile end-user device and application(s). Pet. 24 (citing Ex. 1005, 19:25–34).

Petitioner does not rely on Kalibjian for this aspect of limitation [1.3]. Pet. 20–23. Moreover, Dr. Traynor's declaration does not help Petitioner because Dr. Traynor merely repeats the Petition's assertions with respect to limitation [1.3], without providing additional detail or explanation. Ex. 1003 ¶¶ 46–48; *see* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Consequently, Petitioner has failed to demonstrate a reasonable likelihood that claim 1 is unpatentable over the combination of Houghton and Kalibjian.

4. Claims 3–13

Petitioner contends that dependent claims 3–13, which are dependent on claim 1, are unpatentable over Houghton in view of Kalibjian. Pet. 31–50. Because Petitioner has failed to demonstrate a reasonable likelihood that independent claim 1 is unpatentable based on this combination, Petitioner has also failed to establish a reasonable likelihood that claims 3–13, which are dependent on claim 1, are unpatentable based on the same combination.

E. Grounds 1B and 1C

In Ground 1B, Petitioner contends that claims 2 and 16–18, which depend from claim 1, would have been obvious over the combination of Houghton, Kalibjian, and Munson. Pet. 51–58. In Ground 1C, Petitioner contends that claims 14 and 15, which depend from claim 1, would have been obvious over the combination of Houghton, Kalibjian, and Rakic. *Id.* at 58–65. In Grounds 1B and 1C, Petitioner does not rely on Munson or

Rakic to cure the defects identified in limitation [1.3] for Ground 1A. Because Petitioner has failed to demonstrate a reasonable likelihood that independent claim 1 is unpatentable in Ground 1A, Petitioner has also failed to establish a reasonable likelihood that claims 2 and 14–18 are unpatentable in Grounds 1B and 1C.

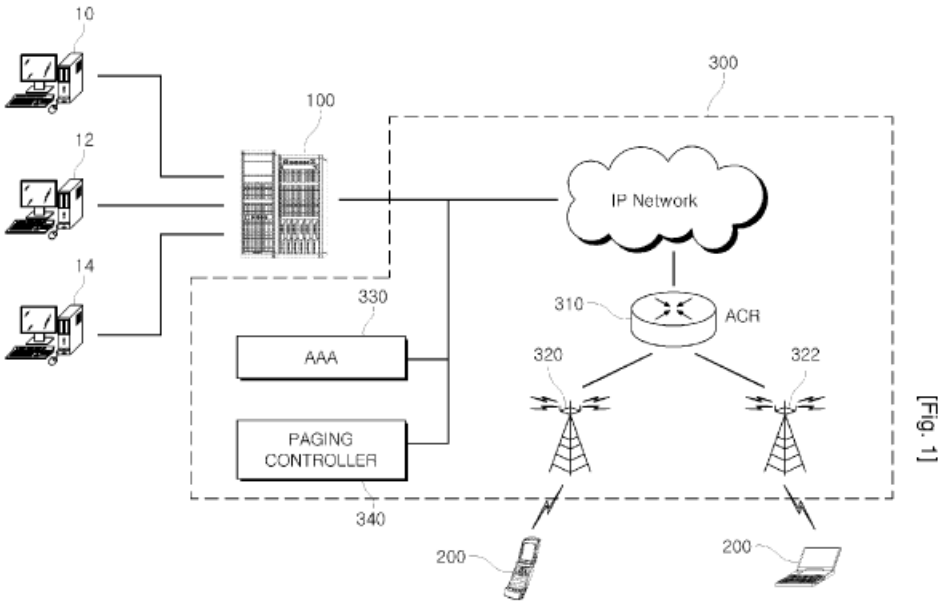
F. Ground 2A: Asserted Obviousness of Claims 1, 3–6, 9–11 and 13–15 Based on Lee, Ellison, and Anderson

Petitioner contends that claims 1, 3–6, 9–11, and 13–15 would have been obvious over Lee in view of Ellison and Anderson. Pet. 65–94. Patent Owner disagrees, arguing that Petitioner has failed to establish that these claims would have been obvious based on this combination. Prelim. Resp. 16–28.

1. Overview of Lee (Ex. 1012)

Lee discloses "a system and a method for providing an integrated push service in an internet service network." Ex. 1012, code (57). This system includes "a plurality of push application servers for providing . . . push information," which includes "push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data." *Id.* The system also includes "an integrated push service server for receiving the push information" and providing it "to the mobile terminal receiving the push data." *Id.* Lee's mobile terminal includes "a communication session manager resident in a memory," which maintains "a communication session with the integrated push service server." *Id.*

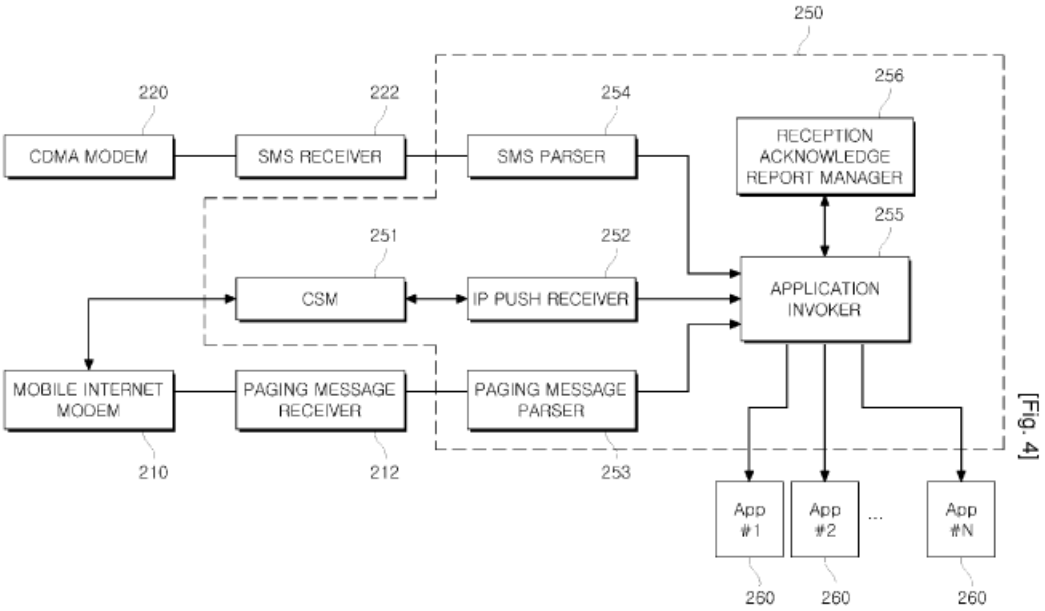
An overview of Lee's integrated push service system is shown in Figure 1, reproduced below.



Lee's Figure 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the invention. Ex. 1012 ¶ 16, Fig. 1.

As shown in Figure 1, Lee's integrated push service system includes "a plurality of push application servers 10, 12, and 14, an integrated push service server 100, a mobile internet service network 300, and a mobile terminal 200 including an integrated push service agent 250." Ex. 1012 ¶ 22. Push application servers 10, 12, and 14 provide push data to a push service application stored in the mobile terminal 200. *Id.* For example, the push data may include "real time news data for a news application, a chatting message for a peer-to-peer messenger application, or an e-mail message for an e-mail application." *Id.* The push data can also include push information "including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and an associated application ID app_ID specifying the application for invoking the push data." *Id.*

Lee's integrated push service agent 250 is illustrated in Figure 4, reproduced below.



Lee's Figure 4 is a diagram illustrating an integrated push service agent 250 in accordance with an embodiment of the invention. Ex. 1012 ¶ 19, Fig. 4.

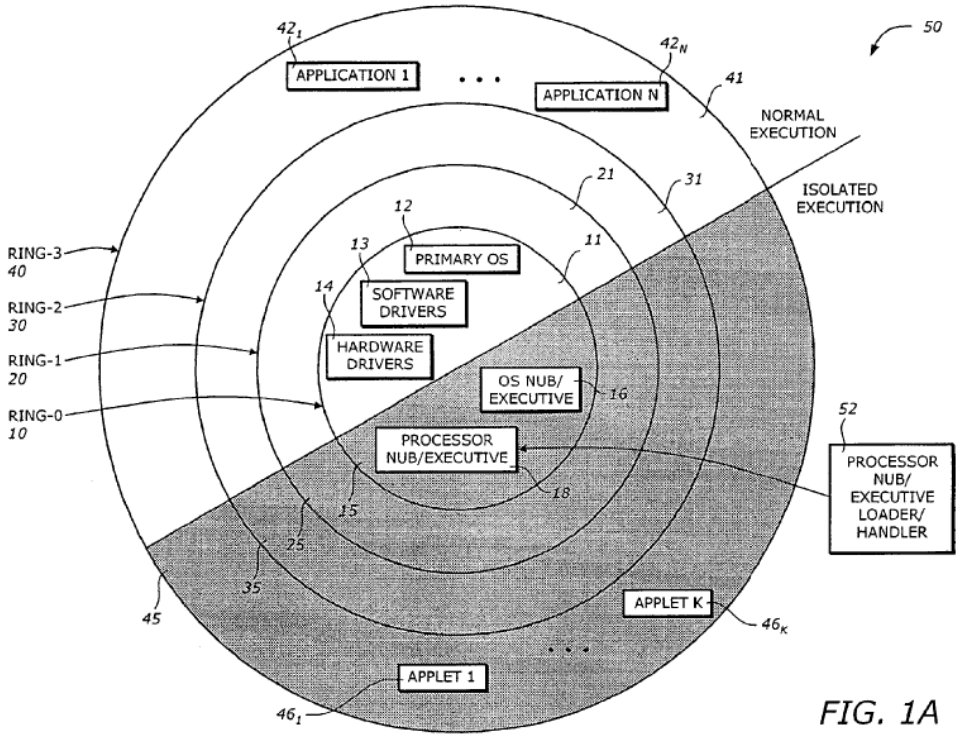
As shown in Figure 4, integrated service agent 250 in mobile terminal 200 receives the push information through mobile internet modem 210, and includes at least one application 260 that is to be associated with the push information. Ex. 1012 ¶ 28. Integrated Service agent 250 receives push information from mobile internet modem 210, which is connected to mobile internet service network 300, and uses this information to selectively invoke the application 260 that corresponds to the associated application ID (app_ID) in the push information. *Id.*

2. Overview of Ellison (Ex. 1013)

Ellison discloses "a method and apparatus to protect a subset of a software environment," in which "[a] key generator generates an operating system nub key (OSNK)," which is "unique to an operating system (OS)

nub." Ex. 1013, code (57). The OS nub "is part of an operating system in a secure platform." *Id.* A "usage protector" uses the OSNK to "protect usage of a subset of the software environment." *Id.*

Ellison explains that "[o]ne principle for providing security in a computer system or platform is the concept of an isolated execution architecture," which "includes logical and physical definitions of hardware and software components that interact directly or indirectly with an operating system of the computer system or platform." Ex. 1013, 2:41–46. The system "may have several levels of hierarchy, referred to as rings, corresponding to various operational modes." *Id.* at 2:46–49. These rings are part of a logical operating architecture 50, as shown in Ellison's Figure 1A, reproduced below.



Ellison's Figure 1A is a diagram illustrating a logical operating architecture including multiple levels of hierarchy, shown as rings, corresponding to various operational modes. Ex. 1013, 1:57–59, 2:46–51, Fig. 1A.

Referring to Figure 1A, Ellison explains that a ring "is a logical division of hardware and software components that are designed to perform dedicated tasks within the operating system," which "is typically based on the degree or level of privilege, namely the ability to make changes to the platform." *Id.* at 2:49–53. For example, according to Ellison, "a ring-0 is the innermost ring, being at the highest level of the hierarchy," which "encompasses the most critical privileged components." *Id.* at 2:53–56. By contrast, "Ring-3 is the outermost ring, being at the lowest level of the hierarchy," and "typically encompasses users or applications level and has the least privilege." *Id.* at 2:57–60. Ellison further explains that "[t]he logical architecture 50 has two modes of operation: normal execution mode and isolated execution mode." *Id.* at 3:4–6.

Ellison's Figure 1B is a diagram illustrating the accessibility of various elements in the operating system and processor according to an embodiment of the invention.

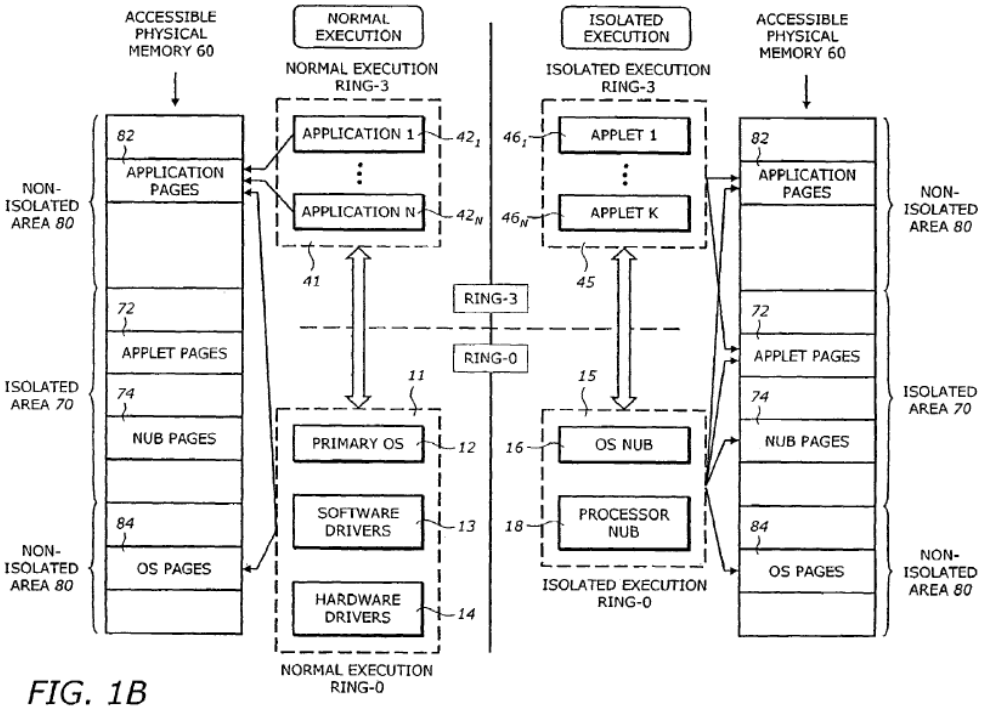


FIG. 1B

Ellison's Figure 1B is a diagram illustrating a secure platform according to one embodiment of the invention.
Ex. 1013, 1:61–63.

Ellison explains that Figure 1B shows how "[t]he various elements in the logical operating architecture 50 access an accessible physical memory 60 according to their ring hierarchy and the execution mode." Ex. 1013, 4:12–14. Accessible physical memory 60 "includes an isolated area 70," which "includes applet pages 72 and nub pages 74" and a "non-isolated area 80," which "includes application pages 82 and operating system pages 84." *Id.* at 4:14–19. Isolated area 70 "is accessible only to elements of the operating system and processor operating in isolated execution mode." *Id.* at 4:19–21. "[N]ormal execution ring 3, including applications 42_i to 42_N, can access only . . . application pages 82" and "cannot access the isolated area 70." *Id.* at 4:26–29.

Ellison's Figure 2 shows an illustration of a secure platform in accordance with one embodiment of the invention.

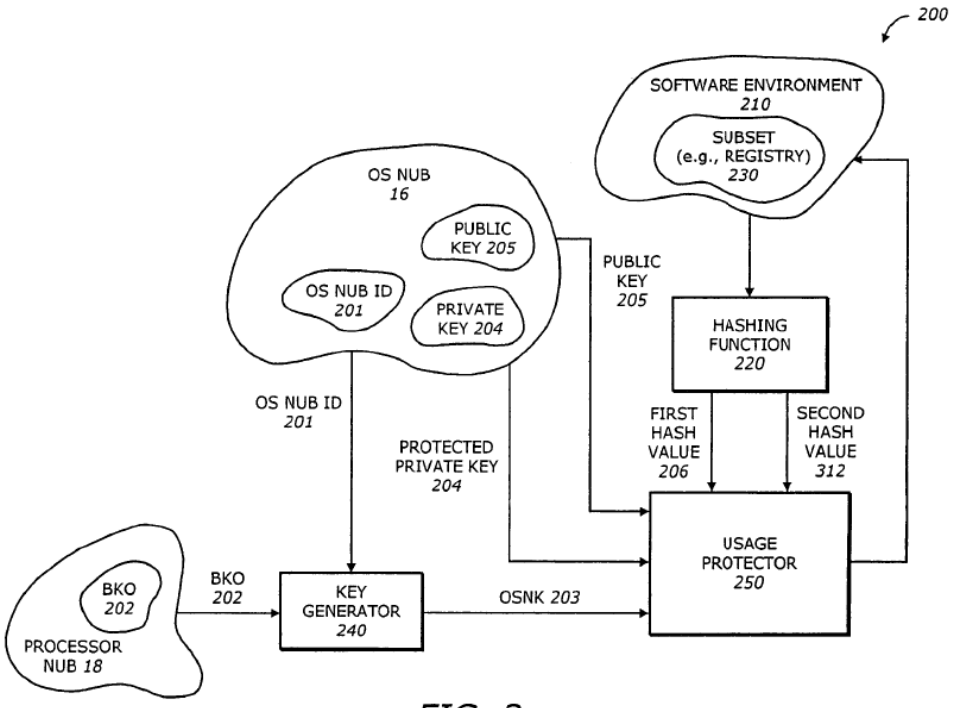


FIG. 2

Ellison's Figure 2 is a diagram illustrating a secure platform according to one embodiment of the invention. Ex. 1013, 1:65–66, Fig. 2.

As shown in Figure 2, Ellison's secure platform 200 includes OS nub 16, processor nub 18, key generator 240, hashing function 220, and usage protector 250, all operating within an isolated execution environment. Ex. 1013, 8:25–32. Secure platform 200 also includes software environment 210 that may exist either inside or outside the isolated execution environment. *Id.*

As Ellison explains, OS nub 16 "is part of the operating system running on the secure platform 200," and "has an associated OS nub identifier (ID) 201, that may be delivered with the OS nub 16 or derived from an OS nub code or associated information." Ex. 1013, 8:33–37. Processor nub 18 "includes a master binding key (BK0) 202," which "is generated at random when the processor nub 18 is first invoked, i.e., when it

is first executed on secure platform 200." *Id.* at 8:66–9:2. "Key generator 240" generates an "operating system nub key (OSNK) 203 which is provided only the OS Nub 16" and may be supplied "to trusted agents, such as the usage protector 250." *Id.* at 9:2–6. Key generator 240 "generates the OSNK 203 by combining the BK0 202 and the OS Nub ID 201 using a cryptographic hash function." *Id.* at 9:9–11.

Software environment 210 "may include a plurality of subsets (e.g., subset 230)," and the usage of software environment or subset 230 "is protected by the usage protector 250," which "uses the OSNK 203 to protect the usage of the subset 230." Ex. 1013, 9:27–32. Subset 230 "is hashed by the hashing function 220 to produce a first hash value 206 and a second hash value 312." *Id.* at 9:39–40. Ellison explains that "[o]ne way to detect intrusion or modification of the subset 230 is to compare the state of the subset before and after a time period" by comparing the first and second hash values. *Id.* at 9:41–45. "If the two hash values are not the same," usage protector 250 "knows that there is a change in the subset 230," and "may generate an error or a fault function" informing the user that "the subset 230 has been tampered, modified" so that "[t]he user may take appropriate action." *Id.* at 9:50–60.

3. Overview of Anderson (Ex. 1010)

Anderson is a textbook entitled "Security Engineering," written by Ross Anderson, a Professor in Security Engineering at Cambridge University. Ex. 1010, 3. Anderson describes security solutions on many platforms, including "Telecom [s]ystem[s]," and describes various examples of secure internet protocols. *Id.* at 9, 21, 26–109.

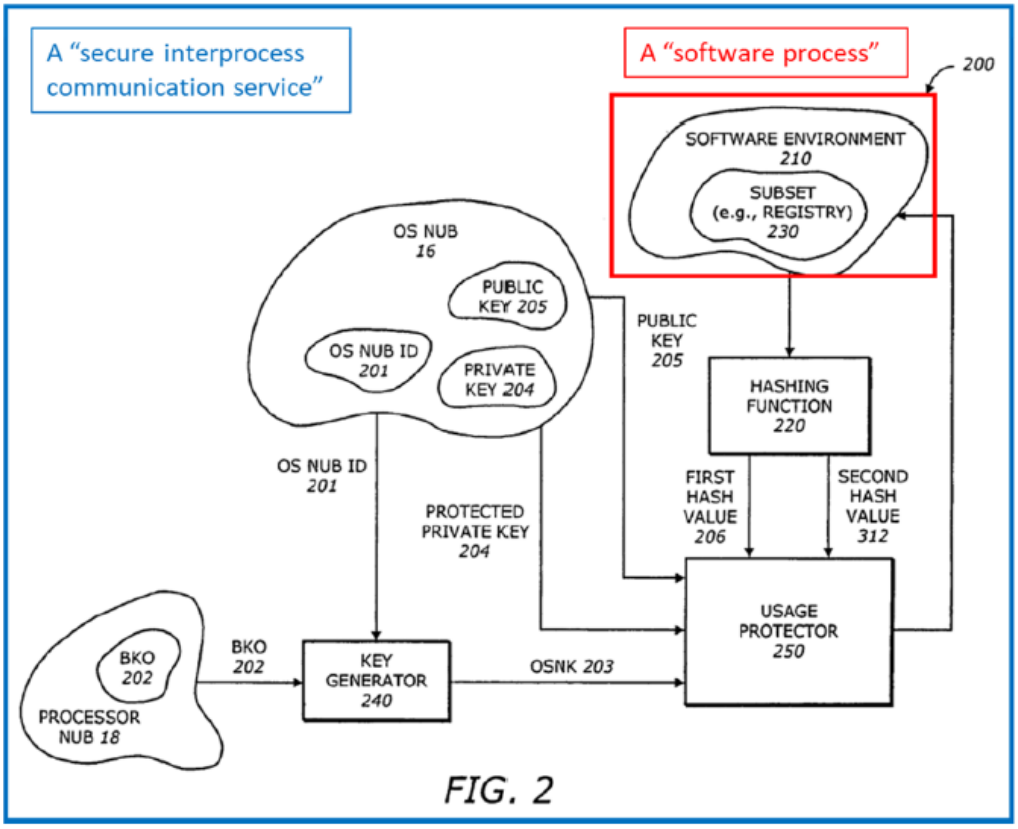
4. Analysis of Independent Claim 1

The parties dispute whether the proposed combination teaches limitation [1.7] of claim 1, which recites that the system, "for each received message, map[s] the application identifier in the message to a software process corresponding to the application identifier, and forward[s] the application data in the message to the software process via a secure interprocess communication service." Ex. 1001, 164:11–15.

Petitioner argues that Lee discloses push service agent 250 (a "device messaging agent") operating on mobile terminal 200 ("executable on a respective one of a plurality of mobile end-user devices") that "maintains [a] communication session with the integrated push service server 100" ("configured to exchange Internet data via a data connection to wireless network") and "selectively invokes the application 260 . . . of the push information . . . to deliver the push data." Pet. 74 (citing Ex. 1012 ¶¶ 25, 28, 29, 34, 44, 49–52, Figs. 1, 4; Ex. 1003 ¶ 124) (emphasis omitted, alterations in original). Petitioner asserts that Lee's push service agent "selectively invokes the application 260 compliant to the associated application ID app_ID of the push information push_info," which corresponds to the claim language requiring that the system "map the application identifier in the message to a software process corresponding to the application identifier." *Id.* at 83 (citing Ex. 1012 ¶¶ 28, 29; Ex. 1003 ¶¶ 134, 135) (emphasis omitted).

Petitioner argues that Ellison discloses an "isolated area 70," which is a "memory area that is defined by the processor 110 when operating in [an] isolated execution mode." Pet. 83 (citing Ex. 1013, 6:1–26, 8:25–32, Figs. 1A–1C, 2). According to Petitioner, "Ellison refers to this technique" as a "secure platform," and Petitioner maps this "secure platform" to the

claim language requiring "a secure interprocess communication service." *Id.* (citing Ex. 1013, 8:25–32, 8:66–67, 9:1–6, 9:28–62, Fig. 2). Petitioner includes an annotated version of Ellison's Figure 2, reproduced below, to illustrate this mapping.



Petitioner's annotated version of Ellison's Figure 2 showing its mapping of software environment 210 (and subset 230) to the claimed "software process" and secure platform 200 to the claimed "secure interprocess communication service." Pet. 84.

Petitioner asserts that Ellison's "secure platform" includes "a 'key generator 240' that 'generates a[n] . . . operating system nub key (OSNK) 203,' which is then supplied to trusted agents." Pet. 83–84 (citing Ex. 1013, 8:66–9:6). "One example of a trusted agent" in Ellison, Petitioner contends, "is a 'usage protector 250' that 'uses the OSNK 203 to protect the usage of [a] subset 230,'" which Petitioner maps to the claim language reciting "a

software process corresponding to the application identifier." *Id.* at 84 (citing Ex. 1013, 9:28–40, Fig. 2) (alteration in original). Additionally, Petitioner argues that "Ellison's usage protector 250 uses a hashing function with the subset 2[30]'s[8] ONSK 203 to determine if the subset 2[30] has been altered following changes (e.g., reads or writes to the subset 2[30]), thereby providing 'protection against unauthorized reads, and detection of intrusion, tampering or unauthorized modification.'" *Id.* (citing Ex. 1013, 9:47–62; Ex. 1003 ¶¶ 135, 136).

Petitioner further argues that, "[i]n the combined Lee-Ellison system," Ellison's "secure platform would have been incorporated into Lee's mobile terminals." Pet. 70 (citing Ex. 1012 ¶¶ 22–29, Figs. 1–2; Ex. 1013, 8:25–32, 8:66–67, 9:1–6, 9:28–62, Fig. 2; Ex. 1003 ¶ 116). More specifically, Petitioner asserts, in implementing the combination, "Lee's push service agent 250 would have forwarded push messages to applications, and Ellison's usage protectors would have protected the recipient applications against unauthorized access or modification," which meets the claim language requiring that the device messaging agent "forward the application data in the message to the software process via a secure interprocess communication service." *Id.* at 85 (citing Ex. 1012 ¶¶ 28, 29; Ex. 1013, 8:25–32, 8:66–67, 9:1–6, 9:28–62, Fig. 2; Ex. 1003 ¶ 137) (alteration in original). "Accordingly," Petitioner contends, "Ellison's secure platform would have provided protection for applications receiving push messages in

[8] The Petition refers to "subset 203," but this appears to be a typographical error because Ellison's Figure 2 refers to "subset 230," not "subset 203." Pet. 84; Ex. 1013, Fig. 2.

Lee's push message system (e.g., malware contained within a push message would be detected using the usage protector 250's hashing function)." *Id.*

Patent Owner responds that the proposed combination fails to teach that each device messaging agent "forward[s] the application data in the message [received from the secure Internet data connection] to the software process via a secure interprocess communication service." Prelim. Resp. 16–28. Patent Owner argues that, for the "secure interprocess communication service" language of limitation [1.7], the Petition relies on Ellison's "isolated area 70," which is "a memory that is defined by [a processor] when operating in [an] isolated execution mode." *Id.* at 17 (citing Pet. 83) (alteration in original). However, according to Patent Owner, "Ellison's 'isolated area 70' is unable to forward data to ***any*** application," as the claim requires, "because Ellison teaches that all applications are prevented from accessing isolated memory area 70." *Id.* (citing Ex. 2001 ¶¶ 47, 48). More specifically, Patent Owner asserts, "Ellison teaches that ***each*** application within its system (Application 1 through Application N) resides in the ring-3 'normal execution' zone," which "cannot access isolated area 70." *Id.* at 17–18 (citing Ex. 1013, 4:26–29, Fig. 1A). Furthermore, according to Patent Owner, the Petition does not argue that it would have been obvious to modify Ellison such that applications would not operate in the "normal execution" zone. *Id.* at 18 (citing Pet. 88–89).

Patent Owner also argues that Petitioner does not establish (or even allege) that Ellison's "secure platform" is used to forward application data to applications. Prelim. Resp. 18. Relying on the testimony of Dr. Brogioli, Patent Owner asserts that one of ordinary skill "would understand that Ellison's secure platform is simply a system to monitor against unauthorized

data accesses, not a platform for secure communication / forwarding of data, roughly akin to how antivirus software monitors malicious activity such as unauthorized changes to application behavior." *Id.* at 18–19 (citing Ex. 2001 ¶¶ 50–54). Referring to Ellison's Figure 2, Patent Owner argues that Ellison's "secure platform" includes "the OS nub 16, the processor nub 18, a key generator 240, a hashing function 220, and a usage protector 250, all operating within the isolated execution environment, as well as a software environment 210," including subset 230, "that may exist either inside or outside the isolated execution environment." *Id.* at 19 (citing Ex. 1013, 8:22–32, 9:28–29). "The ultimate goal of this secure platform," according to Patent Owner, "is to allow usage protector 250 to protect software environment 210 and/or subset 230 from intrusion or modification," which it does by "taking one hash value of subset 230 at a first time, taking a second hash value of subset 230 at a second time, and comparing the hash values to see if there has been an unauthorized access to subset 230 in the duration of time between the hash values." *Id.* at 20–21 (citing Ex. 1013, 9:25–32, 9:50–62; Ex. 2001 ¶¶ 52–53). And, Patent Owner contends, although Ellison describes "several different embodiments of the usage protector 250," these embodiments differ only by "the specific mechanisms by which 'usage protector 250 decrypts the subset' 230." *Id.* at 21 (citing Ex. 1013, 9:63–10:3).

Thus, Patent Owner argues, "Ellison's 'secure platform' of Figure 2 is not a 'communication service,' but instead is a mechanism by which the system can identify unwanted system changes." Prelim. Resp. 21 (citing Ex. 2001 ¶ 54). According to Patent Owner, "Ellison's 'secure platform' is not used to ***forward*** data at all." *Id.* Instead, Patent Owner asserts, "the

Petition alleges only that Ellison's secure platform would have protected ***applications*** from malware, rather than providing security via a communications service through which the malware would be ***forwarded*** to an application (as the limitation [1.7] would require under [the] Petition's theory)." *Id.* (citing Pet. 85). Relying on Dr. Brogioli, Patent Owner contends that Petitioner's "proposed solution would not create security for whatever communications service (such as a communications bus) was used to ***forward*** the push data, but would instead only protect the application from potential security risks that might occur ***after*** the push data had already been received by the application." *Id.* at 22 (citing Ex. 2001 ¶¶ 55–56). Thus, according to Petitioner and Dr. Brogioli, one of ordinary skill "would recognize a difference between the claims of the '117 Patent—which recite a secure 'communication service'—and the disclosures of Ellison which relate to the security of a process that may send or receive data over a communication service (such as an application that might receive malicious data over an unsecured system bus)." *Id.* (citing Ex. 2001 ¶ 57).

Patent Owner also provides an analogy, arguing that Ellison is akin to "a computer downloading an executable file over an unsecured public communications channel (such as public Wi-Fi)," which would not "download data 'via a secure communication service.'" Prelim. Resp. 22 (citing Ex. 2001 ¶ 57). Under this analogy, Patent Owner asserts, "even if strict security protocols (such as extensive antivirus and other security measures) are implemented on the computer receiving the downloaded data," that "does not turn the ***communication service*** used to download the file (i.e., the unsecured public Wi-Fi) into a 'secure communication service.'" *Id.* "In other words," according to Patent Owner, "security

protocols provided at an entity that receives a communication via a communication service are insufficient to turn that communication service into a 'secure communication service.'" *Id.* at 23 (citing Ex. 2001 ¶ 57). Under Petitioner's theory, according to Patent Owner, "data would be forwarded over a 'secure interprocess communication service'—even if the service used to forward the data had no security measures at all—so long as the receiving application had at least some security measures to protect itself against the risks involved in receiving data (including malware) over the unsecure communication service." *Id.* This understanding, Patent Owner contends, is inconsistent with the plain meaning of the claim language reciting that the device messaging agent "forward the application data in the message to the software process via a secure interprocess communication service." *Id.* (citing Ex. 2001 ¶ 56).

Patent Owner further argues that neither the Petition nor Dr. Traynor's declaration "provide[s] any justification for this deviation from plain meaning" or "propose[s] any definition for 'secure interprocess communication service.'" Prelim. Resp. 24 (citing Pet. 83–85; Ex. 1003 ¶¶ 134–137). Patent Owner notes that Dr. Traynor "quotes a portion of the '117 Patent specification relating to an 'interprocess software communication bus' as being relevant to the interpretation of 'secure interprocess communication service,'" but does not "explain[] how that portion of the specification should impact understanding of the claim term." *Id.* (citing Ex. 1003 ¶ 135). In any event, according to Patent Owner, the quoted portion "does not support the Petition's allegation that Ellison's 'isolated area 70' or 'secure platform' constitutes a 'secure interprocess communication service' that is used to forward application data between

processes." *Id.* (citing Ex. 2001 ¶¶ 58–65). Patent Owner argues that the quoted portion of the '117 patent refers to an "interprocess software communication ***bus***," and that "equating a 'communication service' with a 'communication bus' ***undermines*** the invalidity theory of the Petition, because neither Ellison's 'isolated area 70' nor its 'secure platform' are (or are even alleged to be) a communication bus." *Id.* at 24–25 (citing Ex. 2001 ¶¶ 60–61).

Additionally, Patent Owner argues, the quoted portion of the '117 patent discussing a "communication bus" (or a "session bus") does not help Petitioner because "the Petition has not mapped a 'communication bus' or 'session bus' in Ellison (or any other reference for Ground 2) as being a 'secure interprocess communication service.'" Prelim. Resp. 26 (citing Ex. 2001 ¶ 61). Moreover, according to Patent Owner, "the teachings of Ellison on which the Petition relies do not provide for the security of 'communications' over any bus being used to transmit data, and are instead focused [on] the security of applications that could receive data over a bus." *Id.* (citing Ex. 2001 ¶ 64). And, Patent Owner asserts, "[t]he Petition does not even allege Ellison (or any combination involving Ellison) would involve securing, signing, encrypting, or otherwise protecting all communications over a bus." *Id.*

Patent Owner further argues that the portion of the '117 patent quoted by Dr. Traynor, which states that "the session bus can be further protected by ***storing all software . . . in secure memory***, storing all software in encrypted form in secure memory, ***and/or executing all software and communications within a secure execution environment, hardware environment and/or protected memory space***," does not support Petitioner's

position. Prelim. Resp. 26–27 (citing Ex. 1001, 42:58–64) (alteration in original). According to Patent Owner, "Ellison does not (and is not alleged to) disclose 'storing ***all software***' in secure memory (encrypted or otherwise), nor does it disclose 'executing ***all software and communications*** within a secure environment, hardware environment and/or protected memory space.'" *Id.* at 27 (citing Ex. 2001 ¶ 65). "Instead," Patent Owner asserts, "Ellison plainly teaches that a large portion of software is stored and executed ***outside*** of a secure execution environment." *Id.* In support, Patent Owner argues that Figure 1A of Ellison shows "all applications being executed within a 'normal execution' environment, as opposed to other aspects of the system that execute in an 'isolated execution' environment." *Id.* (citing Ex. 1013, Fig. 1A). Also, Patent Owner contends, "Ellison's isolated area and secure platform" do not "relate to executing 'communications' within a secure environment" because "at most those teachings relate to securing a software environment (such as an application) ***after*** the application has already received an unsecure communication." *Id.*

Based on the present record, we determine that Petitioner has failed to make a sufficient showing that the proposed combination teaches the portion of limitation [1.7] requiring that each device messaging agent "forward the application data in the message to a software process via a secure interprocess communication service." First, Petitioner fails to sufficiently show that Ellison's "isolated area 70" discloses or suggests "a secure interprocess communication service." *See* Pet. 83–84. Petitioner states that "isolated area 70" is "[a] memory area that is defined by the processor 110 when operating in [an] isolated execution mode," but fails to explain how this memory area involves the use of a "secure interprocess communication

service." *Id.* at 83 (alterations in original). Moreover, on this record, we agree with Patent Owner and Dr. Brogioli that Ellison teaches that its applications (Application 1 through Application N) reside in the ring-3 "normal execution" zone, which cannot access isolated area 70. Ex. 1013, 4:26–29 (explaining that "[t]he normal execution ring-3, including applications 42_i to 42_N, can access only . . . the application pages 82" and "cannot access the isolated area 70"), Fig. 1A; Prelim. Resp. 17–18; Ex. 2001 ¶ 48. We also find persuasive on this record Dr. Brogioli's testimony that one of ordinary skill "would understand that Ellison's 'isolated area 70' is unable to transfer data to ***any*** application" because "***no*** applications are allowed to access isolated memory area 70." Ex. 2001 ¶ 47.

Petitioner also fails to show that Ellison's "secure platform" discloses or suggests "a secure interprocess communication service." Pet. 83–85. Petitioner relies on Ellison's usage protector 250's use of a hashing function to determine if the subset 230 has been altered following changes (such as reads or writes to the subset). *Id.* at 84. This operation, Petitioner asserts, would have protected applications receiving push messages "against unauthorized access or modification" because "malware contained within a push message would be detected using the usage protector 250's hashing function." *Id.* at 85. Petitioner, however, fails to explain how this use of a hashing function to detect unauthorized access or modification constitutes "a secure interprocess communication service." In this regard, we find persuasive on this record the testimony of Dr. Brogioli that "Ellison's 'secure platform' is not used to forward application data to applications" but instead "is simply a system to monitor against unauthorized data accesses" analogous to "how antivirus software monitors malicious activity such as

unauthorized changes to application behavior." Ex. 2001 ¶ 50. We also find persuasive Dr. Brogioli's testimony that one of ordinary skill "would have recognized that the 'secure platform' of Ellison's Figure 2 is not a 'communication service,' but is instead a mechanism by which the system can identify unwanted system changes" by "check[ing] for suspicious differences in system operation ***after*** data from Lee's push message system had already been forwarded." *Id.* ¶ 54. In this regard, we find helpful Dr. Brogioli's analogy that downloading a file over an unsecured, public Wi-Fi connection to a laptop would not be a "secure communication service" even if antivirus software was installed on the laptop. *Id.* ¶ 57.

We further note that neither Petitioner nor Dr. Traynor provides a claim construction for the term "secure interprocess communication service." Pet. 2–3, 27–31, 83–85; Ex. 1003 ¶¶ 23, 52–54, 134–137. The plain meaning of this term would appear to cover a secure service that communicates between processes. Neither Petitioner nor Dr. Traynor suggests that the term would have a different meaning, or explains how Ellison's secure platform for protecting applications against unauthorized modification would provide a secure service for communicating between processes.

Finally, we note that Dr. Traynor's quotation of a portion of the '117 patent specification discussing an "interprocess software communication bus" does not cure the deficiencies in Petitioner's position. *See* Ex. 1003 ¶ 135 (citing Ex. 1001, 42:45–67, 43:1–4). To begin with, the Petition does not rely on this portion of the '117 patent in discussing the "secure interprocess communication service" limitation. Pet. 83–85. And, neither the Petition nor Dr. Traynor contends that the claim term "secure

interprocess communication service" should be construed to be (or to cover) an "interprocess software communication bus." *Id.* at 2–3, 27–31, 83–85; Ex. 1003 ¶ 135. Moreover, even if the term "secure interprocess communication service" were construed to cover an "interprocess software communication bus," neither Petitioner nor Dr. Traynor points to an "interprocess software communication bus" in Ellison. Pet. 2–3, 83–85; Ex. 1003 ¶¶ 134–137.

Consequently, Petitioner has failed to demonstrate a reasonable likelihood that claim 1 is unpatentable over the combination of Lee, Ellison, and Anderson.

5. Claims 3–6, 9–11, and 13–15

Petitioner contends that dependent claims 3–6, 9–11, and 13–15, which are dependent on claim 1, are unpatentable over Lee in view of Ellison and Anderson. Pet. 85–94. Because Petitioner has failed to demonstrate a reasonable likelihood that independent claim 1 is unpatentable based on this combination, Petitioner has also failed to establish a reasonable likelihood that claims 3–6, 9–11, and 13–15, which are dependent on claim 1, are unpatentable based on the same combination.

G. Grounds 2B and 2C[9]

In Ground 2B, Petitioner contends that claims 2 and 16–18, which depend from claim 1, would have been obvious over the combination of Lee, Ellison, Anderson, and Hämäläinen. Pet. 94–100. In Ground 2C, Petitioner

[9] Petitioner refers to this ground as 2C in the Petition's Table of Contents and discussion of the ground (Pet. ii, 101), but refers to this ground as 3C in its table listing the challenges (*id.* at 1). Because the ground relies on the same combination of Lee, Ellison, and Anderson as Ground 2A, we will refer to this ground as Ground 2C.

contends that claims 7, 8, and 12, which depend from claim 1, would have been obvious over the combination of Lee, Ellison, Anderson, and Houghton. *Id.* at 101–102. In Grounds 2B and 2C, Petitioner does not rely on Hämäläinen or Houghton to cure the defects identified in Petitioner's showing for limitation [1.7] for Ground 2A. Because Petitioner has failed to demonstrate a reasonable likelihood that independent claim 1 is unpatentable in Ground 2A, Petitioner has also failed to establish a reasonable likelihood that claims 2, 7, 8, 12, and 16–18 are unpatentable in Grounds 2B and 2C.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has failed to demonstrate a reasonable likelihood of success in proving that at least one of the challenged claims of the '117 patent is unpatentable. We therefore do not institute trial on any challenged claim raised in the Petition.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), no *inter partes* review of any of challenged claims 1–18 of the '117 patent is instituted with respect to any grounds set forth in the Petition.

IPR2024-00003
Patent 9,198,117 B2

For PETITIONER:

W. Karl Renner
Jeremy Monaldo
Jennifer Huang
FISH & RICHARDSON P.C.
axf-ptab@fr.com
jjm@fr.com
jjh@fr.com

For PATENT OWNER:

Reza Mirzaie
Dale Change
Amy Hayden
James Milkey
Neil Rubin
Philip Wang
RUSS, AUGUST & KABAT
rmirzaie@raklaw.com
dchang@raklaw.com
ahayden@raklaw.com
jmilkey@raklaw.com
nrubin@raklaw.com
pwant@raklaw.com
rak_headwater@raklaw.com